一种隐藏访问结构的文件层次属性加密研究 *

沈学利[a]，吕莹楠[b]

(辽宁工程技术大学 a. 电子与信息工程学院; b. 研究生院, 辽宁 葫芦岛 125105)

摘　要：基于文件层次结构的属性加密方案在云存储环境下是高效率、低存储的，但访问结构本身包含敏感信息，存在用户信息泄露、文件易被窃取的风险，针对这一问题提出了一种隐藏访问结构的文件层次属性加密方案。该方案在不影响加密解密效率的前提下提高了加密算法的安全性，并采用双因子身份认证机制实现了更安全高效的访问控制。该研究成果基于判定性双线性 Diffie-Hellman 假设，在标准模型下被证明是安全的。

关键词：云存储；访问结构；文件层次；属性加密；双因子身份验证

中图分类号：TP391　　doi: 10.3969/j.issn.1001-3695.2017.07.0698

Research on file hierarchy attribute encryption of hidden access structure

Shen Xueli[a], Lyu Yingnan[b]

(*a. School of Electronics & Information Engineering*; *b. School of Graduate Studies Liaoning Technical University*, *Huludao Liaoning* 125105, *China*)

Abstract: The attribute encryption scheme based on file hierarchy is efficient and low in the cloud storage environment, but the access structure itself contains sensitive information, there is the risk of user information leakage and easy to be stolen. Aiming at this problem, this paper proposed a file-level attribute encryption scheme with hidden access structure. The scheme improved the security of the encryption algorithm without affecting the encryption and decryption efficiency, and adopted a two-factor authentication mechanism to achieve a more secure and efficient access control. The results of the study are based on the deterministic bilinear Diffie-Hellman hypothesis, which is proved to be safe under the standard model.

Key Words: cloud storage; access structure; file hierarchy; attribute encryption; two-factor authentication

0　引言

云存储以分布式计算技术为基础，在开放的网络环境下为用户提供了强大的共享和存储能力，然而传统的加密技术已经不能满足用户对于细粒度的访问控制要求[1]。因此 Waters 等人提出了一种基于密文策略的属性加密方案(CP-ABE)[2]实现细粒度的访问控制。已有很多学者提出的一些基于密文策略的属性加密方案[3~7]在加密具有层次结构的文件时是高开销、低效率的。Wang 等人[8]为此提出了一种基于文件层次的属性加密访问控制方案 (简称 FH-CP-ABE)，该方案通过访问结构分层模型来解决多层次文件共享的问题，文件使用一个集成的访问结构进行加密以减少存储成本和计算复杂度，但由于访问结构本身具有敏感信息，对访问结构进行攻击易造成用户信息泄露、文件易被窃取的风险。

在云存储环境下，基于属性加密（ABE）的加密方案可以实现灵活的用户访问控制，其中身份认证是访问控制的第一道防线，是云存储环境安全的基础。双因子身份认证是一种强化的网络访问控制机制，它为登录过程增加了额外的安全层。1999 年 Yang 等人[9]首次提出了一种使用智能卡的密码认证方案，区别于常规的密码方案该方案的关键是首次采用双因子身份验证策略。随后在此方案的基础上一些学者提出了大量关于双因子认证方案，比如 Fan 等人[10]提出的一种强大的远程认证方案与智能卡。Das 等人[11]提出的一种基于动态 ID 的远程用户认定方案,解决静态用户 ID 被攻击的安全问题。2015 年 Wang 等人[12]提出了一种分布式系统中匿名双因子认证机制，该方案是高效的且安全的。

本文为解决上述问题，参考已有的隐藏访问策略的加密模型[13~16]提出一种隐藏访问结构的文件层次属性加密方案（简称 HASFH-CP-ABE）。通过对访问结构进行部分隐藏，防止访问结构泄露敏感信息，造成用户信息泄露，文件被窃取的风险。同时采用文献[12]中的双因子身份验证机制,实现更安全高效的访问控制。

本方案基于判断性 DBDH 假设，在标准模型下被证明是安全的。

基金项目：基于拍卖和域能的企业级虚拟网络映射研究基金项目（61602227）

作者简介：沈学利（1969-），男，江苏连云港人，教授，硕士，主要研究方向为网络安全，计算机网络（523419858@qq.com）；吕莹楠（1993-），女，辽宁阜新人，硕士研究生，主要研究方向为网络安全.

1　相关工作

1.1　双线性映射

G0 和 G1 是两个阶为素数 p 的乘法循环群，g 为 G0 的生成元，双线性映射 e： $G_0 \times G_0 \to G_1$，e 满足以下性质：

(a)双线性。对 $\forall u,v \in G_0$， $a,b \in Z_p$， 都有 $e(u^a,v^b)=e(u,v)^{ab}$ 。

(b)非退化性。存在 $u,v \in G_0$,使得 $e(u,v) \neq 1$ 。

(c)可计算性。对所有 $u,v \in G_0$,存在有效计算 $e(u,v)$ 。

1.2　复杂性假设 DBDH

挑战者基于系统安全参数下，选择阶为素数 p 的群组 G_0,G_1，使得 $a,b,c \in Z_p$ ，$r \in G_1$ ，g 为 G_0 的生成元，判断是否 $r=e(g,g)^{abc}$ 。给定一个算法 B，如果：

$$\left| \begin{array}{l} \Pr\left[B\left(g,g^a,g^b,g^c,e(g,g)^{abc}=0\right)\right] \\ -\Pr\left[B\left(g,g^a,g^b,g^c,r=0\right)\right] \end{array} \right| \geq \varepsilon ,$$

则称 B 解决 DBDH 问题的优势为 ε 。

定义 1　如果没有多项式算法有不可忽略的优势解决 DBDH 问题，则称 DBDH 假设成立。

1.3　访问结构

设 $P=\{p_1,p_2 L\ L\ p_n\}$ 为用户集合，对于集合 A， $A \subseteq 2^P$ 是 2^P 上的一个非空子集，即 $A \subseteq 2^P \setminus \{\varphi\}$ 。如果 $B \in A$ 且 $B \subseteq C$， 那么 $C \in A$，则称 A 为单调的。包含于访问结构 A 中的集合称为授权集合，不包含于 A 中的集合称为非授权集合。

1.4　访问结构树

访问结构树 T 代表一个访问结构，这里本文假设所要共享的文件分成 k 个访问级别，则 $M=\{m_1,m_2 L\ m_k\}$，其中 m_1 代表最高级别，m_k 为最低级别。访问树中的节点用(x,y)表示。叶子节点表示属性，非叶子节点表示阈值，为了便于访问树的使用，本文给出如下定义：

$num_{(x,y)}$, 表示节点(x, y)的孩子节点的个数。

$k_{(x,y)}$，表示节点阈值。若节点为叶子节点时， $k_{(x,y)}$ =1；若节点为非叶子节点时： $k_{(x,y)}$ =1，表示 OR， $k_{(x,y)}$ $=num_{(x,y)}$，表示 AND。

$parent_{(x,y)}$,节点(x,y)的父节点。

(x_i,y_i) ,表示级节点,每个级节点是被集成的访问树的根节点。其中 (x_1,y_1) 表示最高级,从上到下级别依次递减。

$child(x,y)$:表示节点(x,y)的孩子节点。

$att(x,y)$:表示与节点(x,y)相关联的属性。

$index(x,y)$,表示访问树为每个节点的孩子节点任意分配从 1 至 $num_{(x,y)}$ 的数值。$index(x,y)$ 返回与该节点相关的唯一数值。

1.5　双因子身份验证[12]

双因子身份验证的实施需要两个阶段来完成即注册阶段和验证阶段。为了方便描述给出如下定义： S 为远程服务器， A 为用户服务器，哈希函数 $H_i=\{0,1\}^*=\{0,1\}^{l_i}$，i=1,2,3。⇒ 表示安全通道， → 表示普通通道。x 为 S 的私钥，计算 $y=g^x \bmod p$ 。

1) 注册阶段

用户 U_i 选取其身份 ID_i 密码 PW_i，随机字符串 a，则

$$U_i \Rightarrow S:\{ID_i,H_0(a\ PPW_i)\}$$

用户的注册时间为 t, S 选取随机数 b，计算验证参数：

$$M_i=H_0\left(\left(H_0(ID_i)\oplus H(a\ PPW_i)\right)\right)$$

将以下内容存储在存储条目中：

$$\{ID_i,t,a,Honey_List=NULL\}$$

计算：

$$N_i=H_0(a\ PPW_i)\oplus H_0(x\ PID_i\ Pt)$$

具有安全参数的智能卡 SC 则为

$$S \Rightarrow U_i:\{N_i,M_i,y\}$$

2) 验证阶段

用户将智能卡插入读卡器，并且输入身份信息和密码信息 ID_i',PW_i'，SC 执行下列操作：

$$M_i'=\{H_0(H_0(ID_i')\oplus(a\ PPW_i'))\}$$

若 $M_i'=M_i$，SC 选取随机数 d, 计算：

$$Y_1=g^d \bmod p, Y_2=y^d \bmod p$$

$$K=H_0(x\ PID_i\ Pt)=N_i\oplus H_0(a\ PPW_i)$$

$$CID_i=ID_i'\oplus H_0(Y_1\ PY_2)$$

$$CMK_i=(b\ Pk)\oplus H_0(Y_2\ PY_1)$$

$$M_i''=\{H_0(Y_2\ PK\ PCID_i\ PCMK_i)\}$$

$$U_i \to S:\{Y_2,CID_i,CMK_i,M_i''\}$$

根据用户登录请求信息，S 执行以下操作：

计算：

$$Y_2=Y_1^x \bmod p, ID_i=CID_i\oplus H_0(Y_1\ PY_2), K=H_0(x\ PID_i\ Pt)$$

$M_i'''=H_0(Y_1\ PK\ PCID_i\ PCMK_i)$,验证 $M_i'''=M_i''$ 是否成立。若成立 S 随机生成 e,生成临时密钥

$$K_S=Y_1^e \bmod p$$

$$C_1=g^e \bmod p, C_2=H_1(ID_i\ PID_s\ PY_2\ PC_1\ PK\ PK_S)$$
$$S \to U_i:\{C_1,C_2\}$$

接收到来自远程服务器 S 的消息后，SC 执行计算：

$$K_U=C_1^U \bmod p, C_2'=H_1(ID_i\ PID_s\ PY_2\ PC_1\ PK\ PK_U)$$

验证 $C_2'=C_2$ 是否成立。若成立计算：

$$C_3'=H_2(ID_i\ PID_s\ PY_2\ PC_1\ PK\ PK_U), U_i \to S:\{C_3\}$$

S 接受后计算：

$$C_3'=H_2(ID_i\ PID_s\ PY_2\ PC_1\ PK\ PK_S),\text{验证}C_3'=C_3\text{是否成立}$$

若成立，则验证完成用户 U_i 和 S 认证 K_S 为会话密钥。

2　HASFH-CP-ABE 方案构造

本文在文献[8]的基础上，采用双因子身份认证体制，提出了一种 HASFH-CP-ABE 加密方案。

2.1　用户注册

权威机构 S 的私钥为 x，计算 $y=g^x \bmod p$ 作为系统公钥，用户选取随机字符串 a,并且输入身份和密码 ID_i，PW_i 。计算 $H_0(a\ PPW_i)$，将 $\{ID_i,H_0(a\ PPW_i)\}$ 发送给权威机构 S，S 随机选取参数 b，根据用户注册时间 t 进行计算：

$$M_i=H_0\left(\left(H_0(ID_i)\oplus H(a\ PPW_i)\right)\right), N_i=H_0(a\ PPW_i)\oplus H_0(x\ PID_i\ Pt)$$

并将 $\{ID_i, t, a, Honey_List = NULL\}$ 存储在用户数据库中，将 $\{N_i, M_i, y\}$ 保存在智能卡 SC 中。

2.2　加密算法

定义一个双线性映射 $e: G_0 \times G_0 \to G_1$。$G_0, G_1$ 是阶为素数 p 的乘法循环群，g 是生成元，A 表示系统中的属性集合 $A = \{S_1, S_2 L\ L\ S_n\}$，每个属性 S_i 都有 m 个取值，即

$$S_i = \{t_{i,1}, t_{i,2} L\ L\ t_{i,m}\}\ (1 \le i \le n, m = 1, 2, 3 L\ L\ )$$

用户的属性列表 $L = \{l_1, l_2 L\ M_j\}$，$L \subseteq A, l_i \in S_i$。定义两个哈希函数：

$$H_1^*: \{0,1\}^* \to G_0$$
$$H_2^*: \{0.1\}^* \to G_1$$

T 为访问结构 W 对应的的访问结构树，每个访问结构都对应一个访问结构树，其中访问结构树的根节点为 R。

Setup(1^λ)：系统初始化，输入安全参数 λ，为系统中的任一属性值随机选取 $u_{i,j} \in Z_p^*\ (1 \le i \le n, 1 \le j \le m)$。并随机选取 $\alpha, \beta \in Z_p^*$，计算:

$$H = g^\beta, A_{i,j} = g^{u_{i,j}}, Y = e(g,g)^\alpha$$

输出：

$$PK = \{G_0, g, H, A_{i,j}, Y\}(1 \le i \le n, 1 \le j \le m)$$
$$MSK = \{g^\alpha, \beta, u_{i,j}\}(1 \le i \le n, 1 \le j \le m)$$

系统公开公钥 PK，保存主密钥 MSK。

Encrypt(PK, M, T)：为每一个节点(x, y)选取一个多项式 $q_{(x,y)}$，多项式的选取规则如下：从根节点 R 开始，每个节点(x, y)的多项式 $q_{(x,y)}$ 的阶数为 $d_{(x,y)} = k_{(x,y)} - 1$。

根节点 R 的级坐标为 (x_1, y_1)，随机选取 $w \in Z_p$，设置 $q_{(R)}(0) = q_{(x_1,y_1)}(0) = w$，多项式在其他 $d_{(R)}$ 个点的值随机选取来使其定义完整，访问树中除根节点 R 外其他节点 $q_{(x,y)}(0) = q_{parent(x,y)}(index_{(x,y)})$，其他 $d_{(x,y)}$ 个点的值随机定义：

$$q_{child}(0) = q_{(x,y)}(index(child(x,y)))$$

$$child(x,y) = \{child_{(x,y)_1}, chlid_{(x,y)_2} L\ L\ chlid_{(x,y)num_{(x,y)}}\}$$

对于访问树结构 T,本文将每个级节点下的子树中不包含级节点的子树擦除来实现访问结构的隐藏，擦除后的访问结构用 $\bar{T}$ 表示。输入验证参数：

$$\Re(L,W) = \frac{Y^{q_{x_i,y_i}(0)}}{Decrypt(x,y)}$$

每个级节点(x_i, y_i)都是被集成的原访问结构树的根节点，且每个级节点都对应一个级别的密文。计算:

$$C_i = m_i e(g,g)^{\alpha q_{(x_i,y_i)}(0)},\ C_i' = g^{q_{(x_i,y_i)}(0)}$$

集合 Y 为访问结构树中叶子节点的集合，对于任意的 $(x,y) \in Y$ 计算：

$$C_{(x,y)} = H^{q(x,y)(0)}$$
$$C''_{(x,y)} = H_1(att(x,y))^{q_{(x,y)}(0)}$$

设置 X 为传输节点的集合，TN 表示传输节点的孩子节点中代表阈值的节点的集合。计算：

$$\hat{C}_{(x,y)} = Y^{(q_{(x,y)}(0) + q_{child(x,y)}(0))} \times H_2\left(e(g,g)^{\alpha q_{(x,y)}(0)}\right)$$

输出密文：

$$CT = \{\bar{T}, C_{(x,y)}, C''_{(x,y)}, C_i, C_i', \hat{C}_{(x,y)}, \Re\}$$

2.3　身份验证及用户私钥生成

(1)用户登录输入身份信息和登录口令 ID_i', PW_i'

计算 $M_i' = \{H_0(H_0(ID_i') \oplus (a\ PPW_i'))\}$，验证 $M_i' = M_i$ 是否成立，若成立则智能卡 SC 随机选取 d, 计算:

$$Y_1 = g^d \bmod p, Y_2 = y^d \bmod p$$
$$K = H_0(x\ PID_i\ Pt) = N_i \oplus H_0(a\ PPW_i)$$
$$CID_i = ID_i' \oplus H_0(Y_1\ PY_2), CMK_i = (b\ Pk) \oplus H_0(Y_2\ PY_1)$$

用户将 $\{Y_2, CID_i, CMK_i, M_i''\}$ 发送给权威机构 S。

S 执行 $K = H_0(x\ PID_i\ Pt)$，并计算:

$M_i''' = H_0(Y_1\ PK\ PCID_i\ PCMK_i)$ 验证 $M_i''' = M_i''$ 是否成立，若成立则：$C_2 = H_1(ID_i\ PID_s\ PY_2\ PC_1\ PK\ PK_S)$ 并将 C_2 发送给 U_i，U_i 进行计算：

$$C_2' = H_1(ID_i\ PID_s\ PY_2\ PC_1\ PK\ PK_U)$$

验证 $C_2' = C_2$ 是否成立，若成立计算：$C_3' = H_2(ID_i\ PID_s\ PY_2\ PC_1\ PK\ PK_U)$,用户将计算结果返回给 U_i
$C_3' = H_2(ID_i\ PID_s\ PY_2\ PC_1\ PK\ PK_S)$,验证 $C_3' = C_3$ 是否成立，若成立则验证通过, 则执行用户私钥生成算法, 若不通过则返回⊥。

(2) KeyGen(PK,MSK,L):授权中心执行密钥生成算法，随机选取 $r^* \in Z_P^*$。计算:

$$D = g^\alpha H^{r^*} \qquad D_{l_{(i,j)}} = g^{r^*} \times H_1(l_{(i,j)})^{u_{i,j}} \qquad D''_{l_{(i,j)}} = H^{u_{i,j}}.$$

输出私钥:

$$SK = \{D, D_{l_{(i,j)}}, D''_{l_{(i,j)}}\}$$

2.4　解密算法

(1) 验证判断

系统为每个用户的属性分配一个属性分量，解密过程中，用户将自己的属性分量分别代入计算。判断验证参数 $\Re$ 的值，若 $\Re = 1$ 执行下面解密操作，若 $\Re \ne 1$，则系统返回错误标识符⊥。

(2)Decrypt(CT, SK, (x, y))：若 $\Re = 1$，当节点(x, y)为叶子节点时，令 $i = att(x,y)$，如果 $i \notin S$，那么 $Decrypt(CT, SK, (x,y)) = \perp$，若 $i \in S$，定义解密算法如下:

$$Decrypt(CT, SK, (x,y)) = \frac{e(D_{l_{(i,j)}}, C_{(x,y)})}{e(D''_{l_{(i,j)}}, C''_{(x,y)})}$$

$$= \frac{e\left(g^{r^*} H_1(l_{(i,j)})^{u_{i,j}}, H^{q_{(x,y)}(0)}\right)}{e\left(H^{u_{i,j}}, H_1(att(x,y))^{q_{(x,y)}(0)}\right)}$$

$$= \frac{e\left(g^{r^*}, H^{q_{(x,y)}(0)}\right) e\left(H_1(l_{(i,j)})^{u_{i,j}}, H^{q_{(x,y)}(0)}\right)}{e\left(H^{u_{i,j}}, H_1(att(x,y))^{q_{(x,y)}(0)}\right)} = e(g,g)^{r^* \beta q_{(x,y)}(0)}$$

当(x, y)为非叶子节点，(x, y)的所有孩子节点的集合为 Q，对于集合 Q 里的节点，执行解密操作 $Decrypt(CT,SK,Q)$。将所得结果存储在 F_Q 当中，$S_{(x,y)}$ 表示孩子节点集合Q的任意阈值大小。$S_{(x,y)}$ 存在则 $F_Q \neq null$，否则 $F_Q = null$。令 $i = index(Q)$，定义拉格朗日系数：

$$\Delta_{k,s} = \prod_{l \in s, l \notin k} \frac{(x-l)}{(k-l)}, \quad S'_{(x,y)} = \{index(Q) : Q \in S_{(x,y)}\}$$

计算：

$$Decrypt\left(CT, SK, (x,y)\right) = F(x,y)$$

$$= \prod_{Q \in S_{(x,y)}} F_Q^{\Delta_{i,s'_{(x,y)}(0)}} = \prod_{Q \in S_{(x,y)}} \left(e(g,g)^{r^* \beta q_{(Q)}(0)}\right)^{\Delta_{i,s'_{(x,y)}(0)}}$$

$$= \prod_{Q \in S_{(x,y)}} \left(e(g,g)^{r^* \beta q_{(x,y)}(i)}\right)^{\Delta_{i,s'_{(x_k,y_k)}(0)}} = e(g,g)^{r^* \beta q_{(x,y)}(0)}$$

$$A_i = \frac{e(C'_i, D)}{Decrypt\left(CT, SK(x_i, y_i)\right)} = \frac{e\left(g^{q_{(x_i,y_i)}(0)}, g^{\alpha} H^{r^*}\right)}{e(g,g)^{r^* \beta q_{(x_i,y_i)}(0)}}$$

$$= \frac{e\left(g^{q_{(x_i,y_i)}(0)}, g^{\alpha} \times g^{\beta r^*}\right)}{e(g,g)^{r^* \beta q_{(x_i,y_i)}(0)}} = \frac{e\left(g^{q_{(x_i,y_i)}(0)}, g^{\alpha}\right) e\left(g^{q_{(x_i,y_i)}(0)}, g^{\beta r^*}\right)}{e(g,g)^{r^* \beta q_{(x_i,y_i)}(0)}} = e(g,g)^{\alpha q_{(x_i,y_i)}(0)}$$

基于访问树的层次性，如果一个用户的属性集包含低授权节点，那么可以通下面这个公式递归计算出每个授权节点的 A_i 值。计算公式如下：

$$A_{(i+1),j} = \frac{\hat{C}_{(x_i,y_i)}}{A_i \times H_2(A_i)} = \frac{Y^{\left(q_{(x_i,y_i)}(0) + q_{(chil_j)}(0)\right)} \times H_2\left(e(g,g)^{\alpha q_{(x_i,y_i)}(0)}\right)}{e(g,g)^{\alpha q_{(x_i,y_i)}} \times H_2\left(e(g,g)^{\alpha q_{(x_i,y_i)}(0)}\right)}$$

$$= e(g,g)^{\alpha q_{child_j}(0)}$$

得到 A_i 后，利用下列公式获得授权文件：

$$M = \frac{C'_i}{A_i} = \frac{m_i e(g,g)^{\alpha q_{(x_i,y_i)}(0)}}{e(g,g)^{\alpha q_{(x_i,y_i)}(0)}} = m_i$$

3 安全性分析

3.1 抵抗选择明文攻击

定理 1 如果一个概率多项式时间内的敌手 B 没有不可忽略的优势赢得选择性明文攻击下的安全游戏，则该方案是安全的。

证明 构建一个模拟器 B，该模拟器能够以 $\varepsilon/2$ 的优势辨别出 DBDH 元组和随机元组的区别。定义一个有效的可计算的双线性映射 $e: G_0 \times G_0 \to G_1$，随机选取 $l, m, n \in Z_p$，$u \in \{0,1\}$，$R \in G_1$，g 为 G_0 的生成元。挑战者定义一个访问结构树 T，T 的值定义如下：

$$T = \begin{cases} e(g,g)^{lmnc}, u = 0 \\ R, u = 1 \end{cases}$$

模拟器 B 在该游戏中为挑战者，攻击者为 A.这里假设只有一个文件需要被加密。

(1)Initializatton:攻击者 A 选择访问结构 A'，并将 A' 发送给挑战者 B.

(2)Setup：挑战者 B 运行初始化算法，随机选取 $\hat{l} \in Z_p$，定义 $l = \hat{l} + \ln$，$H = g^{\beta} = B = g^{n}$

计算：

$$e(g,g)^{l} = e(g,g)^{\hat{l} + \ln}$$
$$= e(g,g)^{\hat{l}} e(g,g)^{\ln}$$

挑战者 B 将公共密钥 PK 发送给攻击者 A。

(3)Phase 1:攻击者 A 可以自适应性地向挑战者询问私钥提供的属性集：

$S_{i,j} = \{s_{i,j} \in A\} (S_{i,j} \notin A')$ 的私钥 SK。挑战者 B 根据 A 提供的访问结构 A'，随机选择 $r' \in Z_p$，定义 $r = r' - l$。计算：

$$D = g^{l} \times H^{r} = g^{l' + \ln} g^{nr} = g^{l' + nr'}$$

对于每一个属性 $s_{i,j} \in A$，B 为每个属性随机选取 $u'_{i,j} \in Z_p$。计算：

$$D'_{i,j} = g^{(r'-l)} \times H_1(s_{i,j})^{u'_{i,j}} = \frac{g^{r'}}{g^{l}} \times H_1(s_{i,j})^{u'_{i,j}}$$

$$D''_{i,j} = H^{u''_{i,j}} = g^{nu'_{i,j}}$$

最后，挑战者 B 将私钥发送给 A。

(4)Challenge:攻击者 A 提供两个等长的密文消息 m_1 和 m_2，挑战者 B 随机选取 $x \in \{0,1\}$，在访问结构 A' 下，运行加密算法。计算：$\hat{C} = g^{m}$

$$\hat{C}' = m_x e(g,g)^{lm} = m_x e(g,g)^{(\hat{l} + \ln)m} = m_x T e(g,g)^{\hat{l} m}$$

挑战者将密文 CT 发送给攻击者 A。

(5)Phase 2:重复 Phase 1。

(6)Guess:攻击者 A 输出对于 u 的猜想 u'' $(u'' \in \{0,1\})$

如果 $u = u''$，挑战者 B 输出 $u = 0$，那么 $T = e(g,g)^{lmn}$，密文 CT 为有效的，攻击者的优势为 ε，即：

$$\Pr\left[B\left(g, g^{l}, g^{m}, g^{n}, T = e(g,g)^{lmn}\right) = 0\right] = \frac{1}{2} + \varepsilon$$

如果 $u \neq u''$，则输出 $u = 1$，那么 $T = R$，从攻击者的角度来看 $\hat{C}'$ 是完全随机的，因此 $u \neq u''$ 和 $u = u''$ 的概率一样都为 $1/2$，即

$$\Pr\left[B\left(g, g^{l}, g^{m}, g^{n}, T = R\right) = 0\right] = \frac{1}{2}$$

在选择性明文攻击的安全游戏中，B 的优势为

$$Adv_B = \frac{1}{2}\left(\begin{array}{l} \Pr\left[B\left(g, g^{l}, g^{m}, g^{n}, T = e(g,g)^{lmn}\right) = 0\right] + \\ \Pr\left[B\left(g, g^{l}, g^{m}, g^{n}, T = R\right) = 0\right] \end{array}\right) - \frac{1}{2} = \frac{\varepsilon}{2}$$

由上可知挑战者解决 DBDH 问题的优势为 $\varepsilon/2$，在 DBDH 假设下，证明提出的数据共享方案是安全的。

3.2 抵抗用户窜谋攻击

本方案采用双因子身份验证机制，每个用户有其唯一 ID 和登录密码 PW，解密时先进行用户登录，根据验证体制对用户身份进行第一道的判断，提高了攻击者破解合法用户身份信息伪装成合法授权用户的难度。通过身份验证后，用户分别将自己具有的属性私钥分量分别代入进行解密计算，验证用户私钥是否满足访问结构。该方案中用户只能知道自己是否具有访问秘密文件的条件，但不能获知自己能够满足访问结构的具体属

性表达式，这就有效防止了多个非法用户或腐化用户窜谋，结合属性私钥获取解密密钥，获取共享文件，或者低授权用户进行越权盗取高级加密文件的风险。

4　验证

本实验代码基于 pbc-0.5.14 库[17]和 CP-ABE 工具包进行验证。实验结果如图 1、2 所示。

图 1 表示在共享的文件数为固定值的情况下(设 k=4)加密解密所需的时间随属性个数的变化。图 2 表示在属性个数一定的情况下（N=30）加密解密所需的时间随文件个数的变化。对于变化的属性数目和文件个数，属性个数和文件个数的实验仿真数据取值分别为 N={10,15,20,25,30,35,40} 和 k={2,4,6,8}。

由实验验证可知当共享文件数为固定值时，随着属性的增多，本方案在加密时是优于原方案的，但在解密时效果不如原方案。当属性值为固定值时，随着文件个数的增多，本方案在加密解密时的效率与原方案无太大差别。因此改进的方案在提高安全性的同时未对加密解密效率产生过多影响。

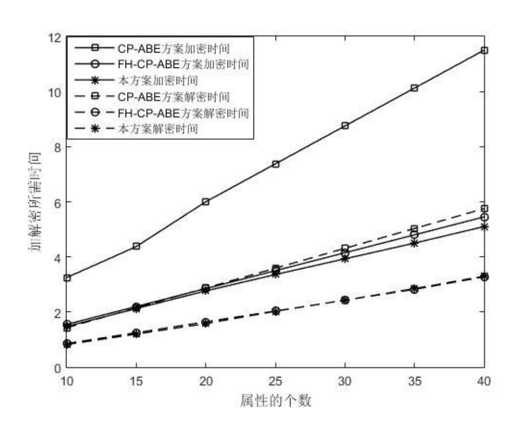


图 1　加/解密时间与属性个数变化关系

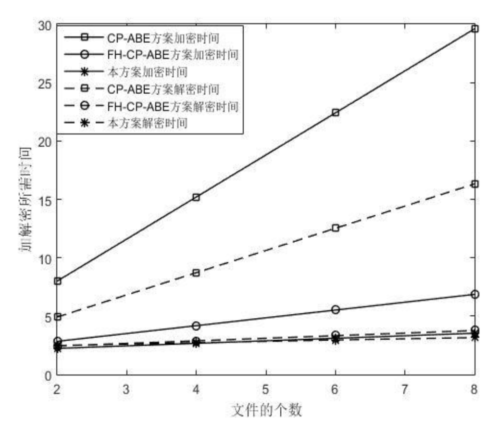


图 2　加、解密时间与文件个数变化关系

5　结束语

通过实验结果验证，本方案在不影响加密解密效率的前提下，解决了用户信息易被泄露、文件易被窃取的风险，并且结合双因子身份认证机制实现对用户身份的匿名认证，使得方案更加高效提高了加密算法的安全性。研究成果在 DBDH 假设下被证明是安全的。

参考文献：

[1] Khalil I M, Khreishah A, Azeem M. Cloud computing security: A survey [J]. IEEE Computers, 2014, 3 (1): 1-35.

[2] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. [J] IEEE Symposium on Security & Privacy, 2007, 2008 (4): 321-334.

[3] Li J, Wang Q, Wang C, et al. Enhancing attribute-based encryption with attribute hierarch [J]. Mobile Net works and Applications, 2011, 16 (5): 553-561.

[4] Wang G J, Liu Q, Wu J, et al. Hierachical attribute-based encryption and scalable user revocation for sharing data in cloud servers [J]. Computers & Security, Advances in Network and Sstem Security, 2011, 30 (5): 320-331.

[5] Hur J. Improving security and efficiency in attribute-based data sharing [J]. IEEE Trans on Knowledge and Data Engineering, 2013, 25 (10): 2271-2282.

[6] Green M, Hohenberger S, Waters B. Outsourcing the decryption of ABE ciphertexts [J]. Usenix Conference on Security, 2011, 49 (3-4): 34-34.

[7] Lai L, Deng H R, Guan C, et al. Attribute-based encryption with verifiable outsourced decryption [J]. IEEE Trans on Information Forensics and Security, 2013, 8 (8): 1343-1354

[8] Wang Shulan, Zhou Junwei, Yu Jianping, et al. A novel file hierarchy access control scheme using attribute-based encryption [J]. Applied Mechanics and Materials, 2015, 701-702: 911-918.

[9] Yang W, Shieh S P. A Password authentication schemes with smart cards [J]. Computers & Security, 1999, 18 (8): 727-733.

[10] Fan C, Chan Y, Zhang Z. Robust remote authentication scheme with smart cards [J]. Elsevier Advanced Technology Publications, 2005, 24 (8): 619-628.

[11] Das M, Saxena A, Gulati V. A dynamic ID-based remote user authentication scheme [J]. IEEE Trans on Consumer Electronics, 2004, 50 (2): 629-631.

[12] Wang Ding, He Debiao, Wang Ping, et al. Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment [J]. IEEE Trans on Dependable & Secure Computing, 2015, 12 (4): 428-442.

[13] Nishde T, Yoneyama K, Ohta K. Attribute-based encryption with partially hidden encryptor-specified access structures [M]. Berlin: Springer, 2008: 111-129.

[14] 解理，任艳丽. 隐藏访问结构的高效基于属性加密方案 [J]. 西安电子科技大学学报, 2015, 42 (3): 97-102.

[15] 宋衍，秦臻，刘凤梅，等. 基于访问树的策略隐藏属性加密方案 [J]. 通信学报, 2015, 36 (9): 119-126.

[16] 李新，彭长根，牛翠翠. 隐藏树型访问结构的属性加密方案 [J]. 密码学报, 2016, 3 (5): 471-479.

[17] Lynn B. The pairing-based cryptography (PBC) library [EB/OL]. http://crypto. Stanford. edu/pbc/.